PAT-NO: JP406195361A

DOCUMENT-IDENTIFIER: JP 06195361 A

TITLE: ELECTRONIC VOTING DEVICE

PUBN-DATE: July 15, 1994

INVENTOR-INFORMATION:
NAME
SAKO, KAZUE
MASUMOTO, HIROYUKI

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NEC CORP	N/A

APPL-NO: JP04292854

APPL-DATE: October 30, 1992

INT-CL (IPC): G06F015/28

ABSTRACT:

PURPOSE: To provide the electronic voting device which can enable voting with out signature in an electronic network and further can prevent illegal voting by providing a key certifying means for an election manager while allocating signature certificate keys and signature secret keys to voting persons.

CONSTITUTION: This non-signature electronic voting system is composed of a preparation phase, tag vote generation phase, voting phase and result open phase. First of all, an election managing center 100 sets a quorum for signature and presents the quorum for signature on an electronic bulletin board 102. The voting person reads the information written on the bulletin

board 102
by using a bulletin board reading means 301, prepares a tag **vote** (t) by using a
tag **vote** preparing means 310, simultaneously prepares a **voting** person signature
secret key (d) and holds it by a signature key holder 312. The center 100
transmits a **blind** signature D to the elector preparing the tag **vote** by using a
blind signature transmitting means 205. A signature preparing means 306
prepares a signature sentence T of the tag **vote** (t) to be certified by the open
key of the center while using the signature D sent from the center 100 and the
quorum for certificate.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－195361

(43)公開日　平成６年(1994)７月15日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ　15/28		Ｂ　8724－5Ｌ		

審査請求　有　　請求項の数５(全 13 頁)

(21)出願番号　特願平4－292854

(22)出願日　平成４年(1992)10月30日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐古　和恵
東京都港区芝五丁目７番１号日本電気株式会社内

(72)発明者　桝本　裕幸
東京都港区芝五丁目７番１号日本電気株式会社内

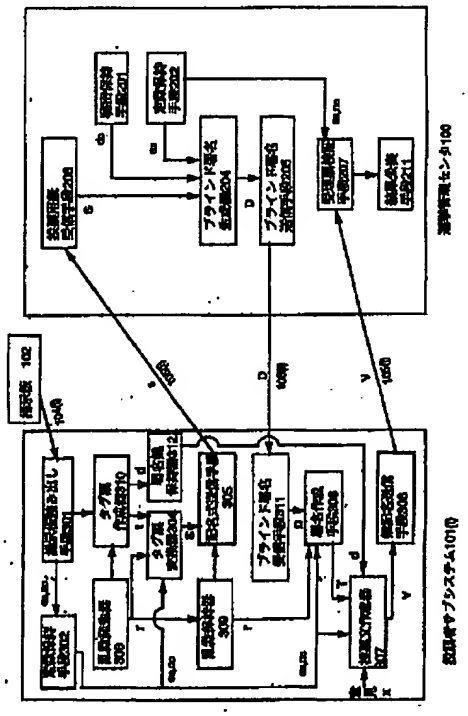
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　電子投票装置

(57)【要約】

【目的】　本発明では、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにできる方式において、同一投票者が２つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない方式を提案することを目的とする。

【構成】　投票者が署名検証鍵と署名秘密鍵を作成し、署名検証鍵をタグ票とするタグ票生成器と、投票者が作成したタグ票に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす投票文作成器と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段からなる。



1

【特許請求の範囲】

【請求項1】　投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、
投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、
投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、
投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、
正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項2】　投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、
投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、
投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、
投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、
正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項3】　投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、
投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、
投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、
投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、
正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項4】　投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、
投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、
投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、
投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、
正当な投票文のみ集計する集計手段を有することを特徴とする電子投票装置。

【請求項5】　請求項1又は3の電子投票装置において、
選挙管理者が無記名で送付された投票文を一方向性関数で変換して公開する公開手段を有することを特徴とする電子投票装置。

2

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は電子ネットワーク上で有権者だけが1度だけ無記名で投票でき、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにできる方式において、同一投票者が2つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない装置を提案することを目的とする。

【0002】

【従来の技術】電子投票方法として従来から知られているものは太田の方法がある。これは特開平1－177164号及び昭和63年電子情報通信学会春季全国大会A－294「単一の選挙管理者を用いた電子投票方式」に開示されている。この方式は投票者は乱数で変換した投票内容に対してセンタの署名を得た後、投票者側で乱数成分を取り除いたもともとの投票内容に対するセンタの署名を作成し、これを無記名でセンタに送ることにより無記名投票を実現している。各投票者は自分の投票が受理・集計されたことを、センタが発表する投票内容一覧で確認する。この方法では自分の意見を反映させた投票内容に対してのみセンタの署名を得られるので、センタがその投票内容を集計しなかった場合、自分の投票内容を公開して異議申し立てを行なわなくてはならない。

【0003】この問題を解決すべく、異議申し立てを行なう場合も、投票者が自分の投票内容を公開せずに異議申し立てを行なうために、あらかじめ投票内容に依存しない投票用紙にのみ署名をもらい、署名付きの投票用紙に自分の意見を反映させた投票内容をセンタに送るという方式が、特願平4－108069号で示された。実施例として各有権者は賛成票・反対票及び投票タグからなる署名つき投票用紙を記名式で入手し、そのうち一方の票を投票タグと共に無記名で投票する方式が述べられている。さらに、不正投票者が2つ以上の意見に投票することを防ぐことを考えた電子投票ほうしきが特願平4－222580号で示された。実施例として投票タグを投票者が生成した署名検証鍵として、各投票者は対応する署名秘密鍵で署名された賛成票・反対票及び投票タグからなる署名つき投票用紙を記名式で入手し、そのうち一方の票を投票タグと共に無記名で投票する方式が述べられている。

【0004】また、1992年電子情報通信学会秋季大会においてA－188「実用的かつ安全な無記名投票方式」が発表された。これは公平性を追及するため、投票者が二度にわたって匿名通信を行う方式である。

【0005】

【発明が解決しようとする課題】特願平4－108069号や特願平4－222580号において、投票用紙の情報量は投票の選択肢の数に比例して大きくなるという問題点がある。たとえば、賛成・反対の2値の投票を行

なう場合には投票用紙は賛成票・反対票・タグ票からなるが、賛成・反対・保留の3 値の投票を行なう場合には投票用紙は賛成票・反対票・保留票・タグ票としなくてはならないように、選択肢が増えるにしたがって通信量や処理量が増加する。さらに、あらかじめ選択肢が固定されていないと投票用紙を作成できず、自由記入形式の投票やアンケートや意見書に対応できないという問題点があった。

【０００６】本発明では選択肢の数が増えても、また選択肢があらかじめ固定されていなくても投票者が１回の匿名通信を用いて効率よく実現できる電子投票装置を提案する。

【０００７】

【課題を解決するための手段】第一の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【０００８】第二の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【０００９】第三の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【００１０】第四の発明の電子投票装置は、投票者が署名検証鍵と署名秘密鍵を作成する鍵生成手段と、投票者が作成した署名検証鍵と投票内容に依存したビット列に対して選挙管理者のブラインド署名を得る鍵認証手段と、投票者が作成した署名秘密鍵を用いて投票内容に署名を施こす署名手段と、投票者の署名つき投票内容と、選挙管理者の署名つき署名検証鍵を暗号化して無記名で選挙管理者に送付する投票手段と、正当な投票文のみ集計する集計手段を有することを特徴とする。

【００１１】第五の発明の電子投票装置は、請求項１又

は３の電子投票装置において、選挙管理者が無記名で送付された投票文を一方向性関数で変換して公開する公開手段を有することを特徴とする。

【００１２】

【実施例】つぎに、図１から図８を参照して第一、第二、第三、第四及び第五の発明の実施例について説明する。

【００１３】本発明の電子投票装置を、図２のように、m個の投票者サブシステム１０１（１）～１０１（ｍ）及び１つの選挙管理センタ１００が相互に安全な通信チャネル（例えばデータ回線）１０５で結ばれており、さらに選挙管理センタ１００のみが書き込み可能な掲示版で、すべての投票者サブシステムが読み出せる電子掲示版１０２が存在する場合の無記名電子投票システムに実施する例を述べる。なお、以下簡単のために選挙管理センタをセンタ、投票者サブシステムを投票者と呼ぶことにする。

【００１４】この投票システムは準備フェーズと、タグ票生成フェーズ、投票フェーズおよび結果公表フェーズからなる。

【００１５】第一及び第三の発明はタグ票生成フェーズ、第二及び第四の発明は投票フェーズ、第五の発明は結果公表フェーズに関する。

【００１６】まず、図３を用いて第一の発明の準備フェーズを説明する。

【００１７】本無記名電子投票システムを実施するための準備として、センタ１００は署名用の定数を設定し、検証用定数を電子掲示版１０２に掲示する。例えば、署名方式としてＲＳＡ暗号方式を用いるとする。そこで、n_c を二つの素数p_c ，q_cの積とし、e_c とd_c を$e_c \cdot d_c = 1 \bmod (p_c - 1)(q_c - 1)$を満たす整数とする。このときセンタは$e_c$ ，n_c を検証用定数として設定する（ステップ１１）。これらの定数を電子掲示版１０２に書き込む（ステップ１２）。今後この検証用定数e_c ，n_c は頻繁に用いられるので自分の定数保持手段２０１に書き込み容易にアクセスできるようにする（ステップ１３）。一方、d_c は自分の秘密情報保持手段２０２に格納する（ステップ１４）。

【００１８】次に、センタ１００は投票に関する規則を定める。まず、投票対象の議題を明らかにする。次に投票フォーマットとしてタグ票フォーマットと投票内容フォーマットを定める。たとえば、以下のようなタグ票フォーマットを考える。このとき、ｅとｎと

【００１９】

ハッシュ値h（e‖n）

【００２０】の連結で、数字としてn_c より小さくなるようなものをタグ票とする。たとえば、関数ｈの出力を６４ビット、ｅを１０ビット、ｎを５１２ビットと定め、あらかじめn_c を５８７ビットに設定すればよい。

【００２１】また、投票内容フォーマットとしては以下

5

が考えられる。投票内容xと乱数yを連結した

【0022】

$$x \| y$$

【0023】と、その

【0024】

$$\text{ハッシュ値} h(e \| n)$$

【0025】を連結したもの

【0026】

$$x \| y \| h(x \| y)$$

【0027】とする。このとき、投票内容全体としてnより小さいものとする。投票内容xはあらかじめ付与された選択肢番号でもいいし、自由形式に記述した文章をアスキー文字列に置き換えたものでもよい（ステップ15）。

【0028】次に、投票する権利のあるサブシステム（以後、有権者と呼ぶ）の名前を一覧にする（ステップ16）。投票用紙作成及び投票の期限を設定・公表し（ステップ17）、タグ票作成フェーズの開始を合図する（ステップ18）。

【0029】以上が準備フェーズである。

【0030】次に、タグ票作成フェーズ、及び投票フェーズを説明するが、両フェーズとも選挙管理センタ100は各投票者に対して同じ手順を踏むので、特定の投票者サブシステム101（i）に対する手順を例にとって説明を続ける。

【0031】図1に示すように無記名電子投票システムはセンタ100が電子掲示版102に定数及び投票規則を書き込む安全通信チャネル103、投票者101（i）が電子掲示版102に書かれた内容を読み出すための安全通信チャネル104（i）および投票者とセンタが交信するための安全通信チャネル105（i）で構成されている。

【0032】まず、図1を参照しながら投票者101（i）のタグ票作成フェーズを説明する。投票者101（i）は掲示板読み出し手段301を用いて掲示板102に書かれてある内容を読み出し、定数e_c，n_cを定数保持手段302に格納する一方、読み出したフォーマットに沿うようなタグ票tをタグ票作成手段310にて作成する。すなわち、まず2つの素数p，qの積である512ビットの数nを定め、（p－1）（q－1）と互いに素な10ビットの数eをさだめる。これと

【0033】

$$h(e \| n)$$

【0034】を連結させたものをタグ票tとする。すなわち

【0035】

$$t = e \| n \| h(e \| n)$$

【0036】とする。また、同時に

$e \cdot d = 1 \mod (p-1)(q-1)$

となるdを求め、投票者署名秘密鍵として保持する。な

6

お、タグ票作成にあたってフォーマットに必要な乱数成分は乱数発生器303の出力を用いる。

【0037】次に、タグ票変換器304は、乱数発生器303の出力rと定数e_c，n_cを用いて、

【0038】

$$s = t \cdot r^{e_c} \bmod n_c$$

【0039】を計算し、sを出力する。また、このときの乱数発生器303の出力rは乱数保持器309に格納する。sを記名付き交信手段305が安全チャネル105（i）を通じてセンタ100に送信する。

【0040】センタ100はタグ票受信手段206で受信した正当な有権者からのsを受信する。ブラインド署名生成器204は秘密保持手段201、定数保持手段202から読みだしたd_c及びn_cを用いて、

【0041】

$$D = s^{d_c} \bmod n_c$$

【0042】を計算し、出力する。ブラインド署名送信手段205はDを投票者101（i）に送信する。

【0043】タグ票作成を行なったすべての有権者に対して署名を送信すればセンタは投票フェーズに移行することを宣言する。以上がタグ票設定フェーズである。

【0044】次に、投票フェーズを説明する。

【0045】署名作成手段306は、ブラインド署名受信手段311によりセンタ100から受信したDと、定数保持手段302から読み出したe_c，n_cを用いて

【0046】

$$s = D^{e_c} \bmod n_c$$

【0047】が成立するかどうか検証する。確認できれば、乱数保持器309から読み出した整数rと、定数保持手段302から読み出したn_c，e_cを用いて、

$T = D / r \mod n_c$

を計算する。

【0048】なお、このTはセンタの公開鍵e_c，n_cで検証可能なタグ票tの署名文になっている。すなわち、

【0049】

$$T^{e_c} \bmod n_c = t$$

【0050】がなりたっている。センタにはタグ票tそのものを見せずにその署名を入手することをブラインド署名と呼び、一連のタグ票変換器304、ブラインド署名生成器204、署名作成手段306がタグ票認証手段である。なお、タグ票は投票者の署名検証鍵でもあるので、鍵認証手段でもある。

【0051】次に、投票文作成器307において投票文を作成する。まず、投票内容フォーマットに従い、自分の投票内容x を反映させた投票v を以下のように生成する。

【0052】

$$v = x \| y \| h(x \| y)$$

【0053】ここでyは発生器303の出力である。次

に署名鍵保持器から読み出した署名鍵ｄを用いてｖに署名を施す。すなわち、

$v' = v^d \mod n$

を計算する。無記名送信手段３０８はこの署名とブラインド署名で得たタグの署名の対ｖ＝（ｖ’，Ｔ）を送信者名を付記せずにセンタ１００に送出する。

【００５４】センタ１００は、受信したＶのうちＴを読み出し

【００５５】

$$\alpha = t^{e_c} \mod n_c$$

【００５６】を計算する。αは投票者が不正をしていなければ、ｔに等しくなる。αがあらかじめ定められたタグのフォーマットであれば、これと同じタグ票が以前使われているかどうか検証する。使われていなければ、次に投票内容を検証する。すなわち、タグ票から署名検証鍵ｅ，ｎを抽出し、

$\beta = (v')^e \mod n$

を計算する。βは投票者が不正をしていなければ、ｖに等しくなる。βがあらかじめ定められた投票内容のフォーマットであれば、これからｘを抽出し、これを集計する。

【００５７】全員の投票が終了したら、センタは結果を公表する。すなわち、すべてのタグ票と投票文の一覧を掲示板に掲げる。各投票者はその一覧を見て、自分の投票が集計されたかどうかを見ることができる。もし集計されていなければ、集計されていないタグ票を公表することにより、センタの集計洩れを指摘でき、かつこの時他の投票者には自分が何に投票したか知られることはない。

【００５８】次に図５を用いて第二の発明の実施例を説明する。準備フェーズとして、第一の発明の実施例の準備フェーズと同様に行なうが、ステップ１１において、センタはさらにＲＳＡ暗号鍵n_2，e_2，d_2を生成し、ステップ１２において公開鍵e_2，n_2を掲示すると共にステップ１３においてd_2を自分の定数保持手段２０１に書き込むところが付加される。

【００５９】また、タグ票作成フェーズも第一の発明の実施例と同様に行うが、掲示板読み出し手段４０１においてe_2，n_2の読み出し、格納が付加される。

【００６０】投票フェーズも第一の発明の実施例と同様に行なうが、投票フェーズにおいて投票文作成器のの出力Ｖ＝（ｖ’，Ｔ）を入力とした投票文暗号化器４０７をおく。この投票文暗号化器においては、投票文Ｖを以下のように暗号化する。定数保持手段３０２から読み出したn_2，e_2を用いて、

【００６１】

$$V' = (v', T^{e_2} \mod n_2)$$

【００６２】を計算し、無記名送信手段４０８はＶ’＝（ｖ’，Ｔ’）を送信者名を付記せずにセンタ１００に送出する。

【００６３】センタ１００は、受理票検証手段４１７において、受信したＶ’のうちＴ’を読み出し

【００６４】

$$\alpha = ((T')^{d_2} \mod n_2)^{e_c} \mod n_c$$

【００６５】を計算する。αは投票者が不正をしていなければ、ｔに等しくなる。αがあらかじめ定められたタグのフォーマットであれば、これと同じタグ票が以前使われているかどうか検証する。使われていなければ、次に投票内容を検証する。すなわち、タグ票から署名検証鍵ｅ，ｎを抽出し、

$\beta = (v')^e \mod n$

を計算する。βは投票者が不正をしていなければ、ｖに等しくなる。βがあらかじめ定められた投票内容のフォーマットであれば、これからｘを抽出し、これを集計する。

【００６６】公表手段としては、暗号化したままのＶ’を掲示し、各自自分の投票文が集計されているかどうかを検証すればよい。

【００６７】なお、投票文暗号化器407 における投票文の暗号化方法としては、上記以外にｖを暗号化する、ｖ’を暗号化する、あるいは投票文とタグ票のどちらも暗号化するなどの方法がある。

【００６８】次に図６を用いて第三の発明の実施例を説明する。

【００６９】準備フェーズとして、第一の発明の実施例の準備フェーズと同様に行なうが、ステップ１５にてタグ票フォーマットを次のように定める。このとき、ｅとｎと投票内容ｘと

【００７０】

$$\text{ハッシュ値} h(e \| n \| x)$$

【００７１】の連結で、数字としてn_cより小さくなるようなものをタグ票とする。

【００７２】また、タグ票作成フェーズも第一の発明の実施例と同様に行うが、タグ票作成手段６１０にて

【００７３】

$$t = e \| n \| x \| h(e \| n \| x)$$

【００７４】をタグ票として設定する。ここでｘは投票者の意見である。

【００７５】このようにすれば、タグ票生成時に各投票者は自分の意見を盛り込むことになるので、投票フェーズの時に自分の意見を変更することはできない。

【００７６】次に図７を用いて第四の発明の実施例を説明する。

【００７７】準備フェーズとして、第二の発明の実施例の準備フェーズと同様に行なうが、ステップ１５にてタグ票フォーマットを次のように定める。このとき、ｅとｎと投票内容ｘと

【００７８】

$$\text{ハッシュ値} h(e \| n \| x)$$

【００７９】の連結で、数字としてnc より小さくなるようなものをタグ票とする。

【００８０】また、タグ票作成フェーズも第二の発明の実施例と同様に行うが、タグ票作成手段７１０にて

【００８１】

$$t=e\|n\|x\|h(e\|n\|x)$$

【００８２】をタグ票として設定する。ここでxは投票者の意見である。

【００８３】次に図８を用いて第五の発明の実施例を説明する。これは結果公表フェーズに関する。

【００８４】次に図８を用いて結果公表フェーズを説明する。第一の発明の実施例、あるいは第三の発明の実施例のように準備フェーズ、タグ票設定フェーズ、投票フェーズを終えているとし、受理票検証手段２０７を経て受理票とされたものは受理票保持手段８１１に格納されているものとする。また、各投票者は自分の投票文を投票文保持手段９０２に保持しているものとする。

【００８５】ここで、一方向性関数として、ＲＳＡ暗号関数を用いる。

【００８６】センタ１００はまず、一方向性関数生成手段８０２において、ＲＳＡ暗号鍵n_2，e_2を生成する。次に受理票変換手段８０１において、受け取ったすべての受理票とそのタグを（n_2，e_2）で暗号変換を行なう。すなわち、受理票Ｖ＝（ｖ’，Ｔ）に対して、

【００８７】

$$V'=(v',T^{e_2} \bmod n_2)$$

【００８８】とする。変換された受理票ｖ’を受理票公表手段２０８において、公表する。同時に暗号鍵（n_2，e_2）も公表する。

【００８９】各投票者１０１（ｉ）は受理票一覧読み出し手段９１１において、変換された受理票一覧及び暗号鍵（n_2，e_2）を読み出し、検証手段９１２において自分の投票が票及びタグが一覧に含まれていることを確認する。すなわち、投票文保持手段９０２に保持している自分の投票文Ｖを（n_2，e_2）を用いて

【００９０】

$$V'=(v',T^{e_2} \bmod n_2)$$

【００９１】と計算し、これが変換された受理票一覧に含まれるかどうかを確認する。

【００９２】確認できなければ、異議申し立て手段９１３を用いて異議申し立てを行なう。これについては後で詳細に述べる。センタはどの投票者からも異議申し立てがなければ、変換されていない受理票と集計結果を公表する。

【００９３】一方、検証手段９１２において自分の投票が受理されていなければ、異議申し立て手段９１３において、自分のタグ票を公表し、それが正当なタグ票であることと、その変換文が集計されていないことを示す。この主張が確認されれば、異議申し立て者の票が受理されていないと処理される。

【００９４】このように異議を申し立てれば、異議申し立て者が実際はどの意見を投票したのかを明らかにすることなく、自分の票が受理されなかったことを証明することができる。さらに、異議申し立て時には全体の投票結果は暗号化されたままなので、投票結果に対する異議とは区別され、従来の方式の様に異議申し立て者が投票結果が不満で異議を唱えているのではないことが明らかになる。

【００９５】図４を参照すると、いづれの実施例で述べたシステムは、通信処理機能を備えたパーソナルコンピュータ等の端末装置（ＴＭＵ）４０１と、読出し専用記憶装置（ＲＯＭ）４０２と、ランダムアクセス記憶装置（ＲＡｍ）４０３と、乱数発生器（ＲＮＧ）４０４と、シグナルプロセッサ（ＳＰ）４０６と、ＴＭＵ４０１、ＲＯＭ４０２、ＲＡＭ４０３、ＲＮＧ４０４およびＳＰ４０６を相互に接続する共通バス４０５とから構成される。

【００９６】ＲＮＧ４０４は乱数をＳＰ４０６の指令により発生する。これはセンタ１００が定数設定の時に用い、また、各投票者１０１（ｉ）の乱数発生器として用いる。ＲＡＭ４０７にはセンタ１００の場合、定数保持手段２０２あるいは秘密情報保持手段２０１になる。秘密情報はＴＭＵから必要に応じてＲＡＭに格納するようにしてもよい。ＲＯＭ４０７には投票者サブシステム１０１（ｉ）の場合、定数保持手段３０２、乱数保持器３０９などになる。ＲＯＭ内に格納されたプログラムに基づいて、上述の動作を実現する。ＲＡＭ４０３はこれらのステップの実行中に計算途中結果等を一時的に記憶するために用いられる。

【００９７】また、システム１００，１０１（ｉ）は汎用電子計算機等のデータ処理装置やＩＣカードであってもよい。

【００９８】

【発明の効果】以上詳細に説明したように、本発明を用いれば、投票者が自分が何に投票したかを他の投票者に知られることなく不正集計に対して異議申し立てをオープンにでき、同一投票者が２つ以上の選択肢に投票することを検出でき、かつこの検出機構を第三者に悪用されない無記名電子投票装置において、選択肢の数によらず処理量・通信量が一定で、従来方式の最小値（選択肢の数が２の場合）より小さい効率の良い電子投票装置が実現できる。本電子投票装置においては選択肢をあらかじめ定める必要がなく、自由記入式のアンケートにも容易に適用できる。

【図面の簡単な説明】

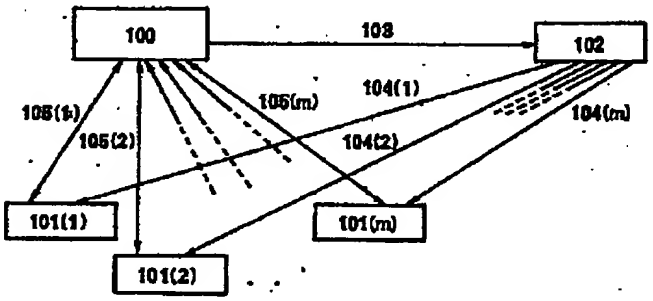
【図１】第一の発明の電子投票装置の一実施例を示すブロック図。

【図２】無記名電子投票システムを示す図。

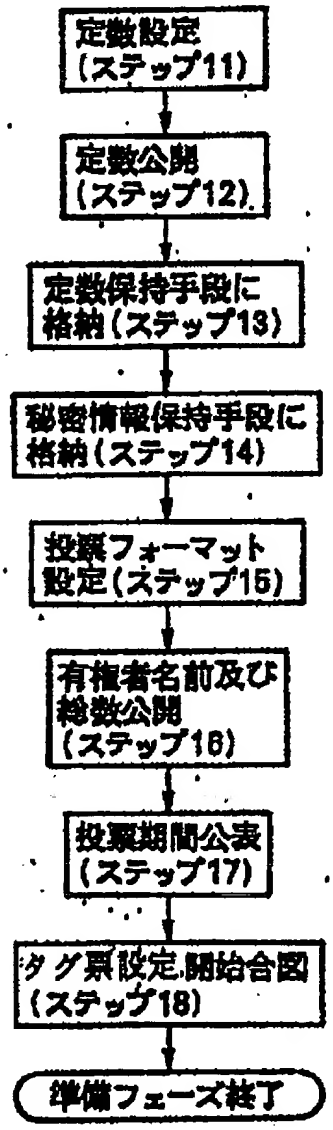
【図３】準備フェーズの例を示す図。

【図4】第一から第五の発明の実施例に用いるシステムの例。
【図5】第二の発明の電子投票装置の位置実施例を示すブロック図。
【図6】第三の発明の電子投票装置の一実施例を示すブロック図。
【図7】第四の発明の電子投票装置の一実施例を示すブロック図。
【図8】第五の発明の電子投票装置の一実施例を示すブロック図。
【符号の説明】
100　選挙管理センタ
101（i）　投票者サブシステム
102　電子掲示板

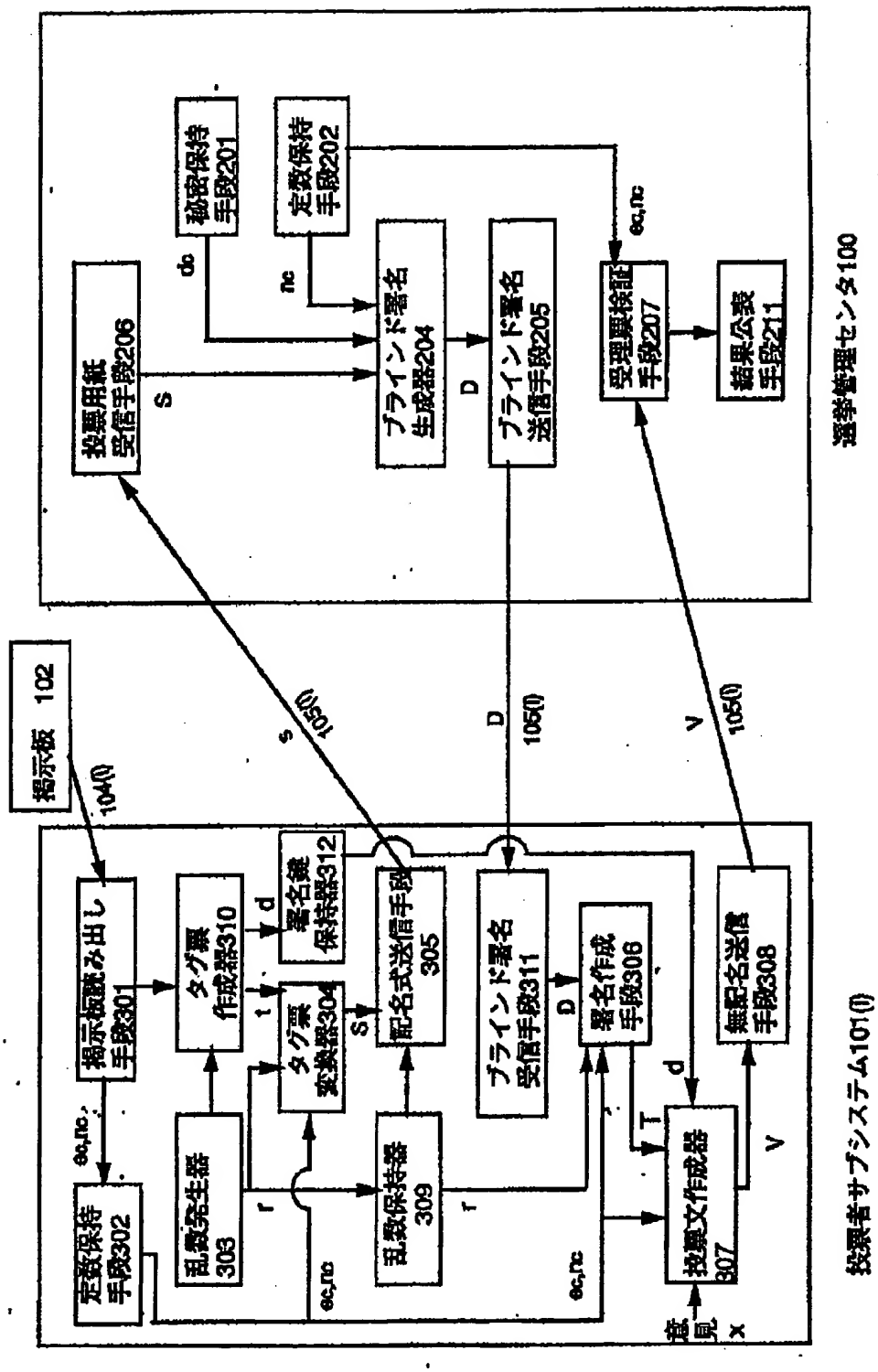
【図2】



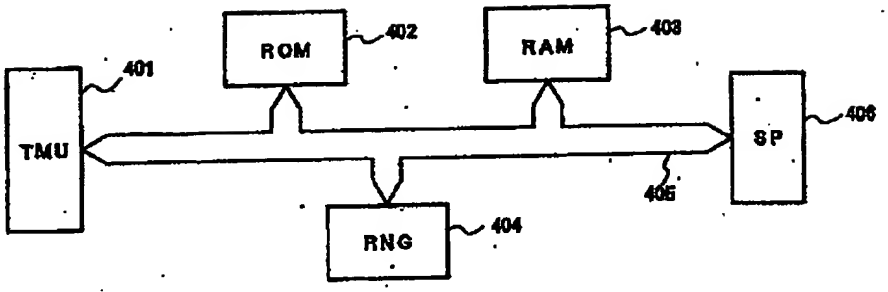
【図3】



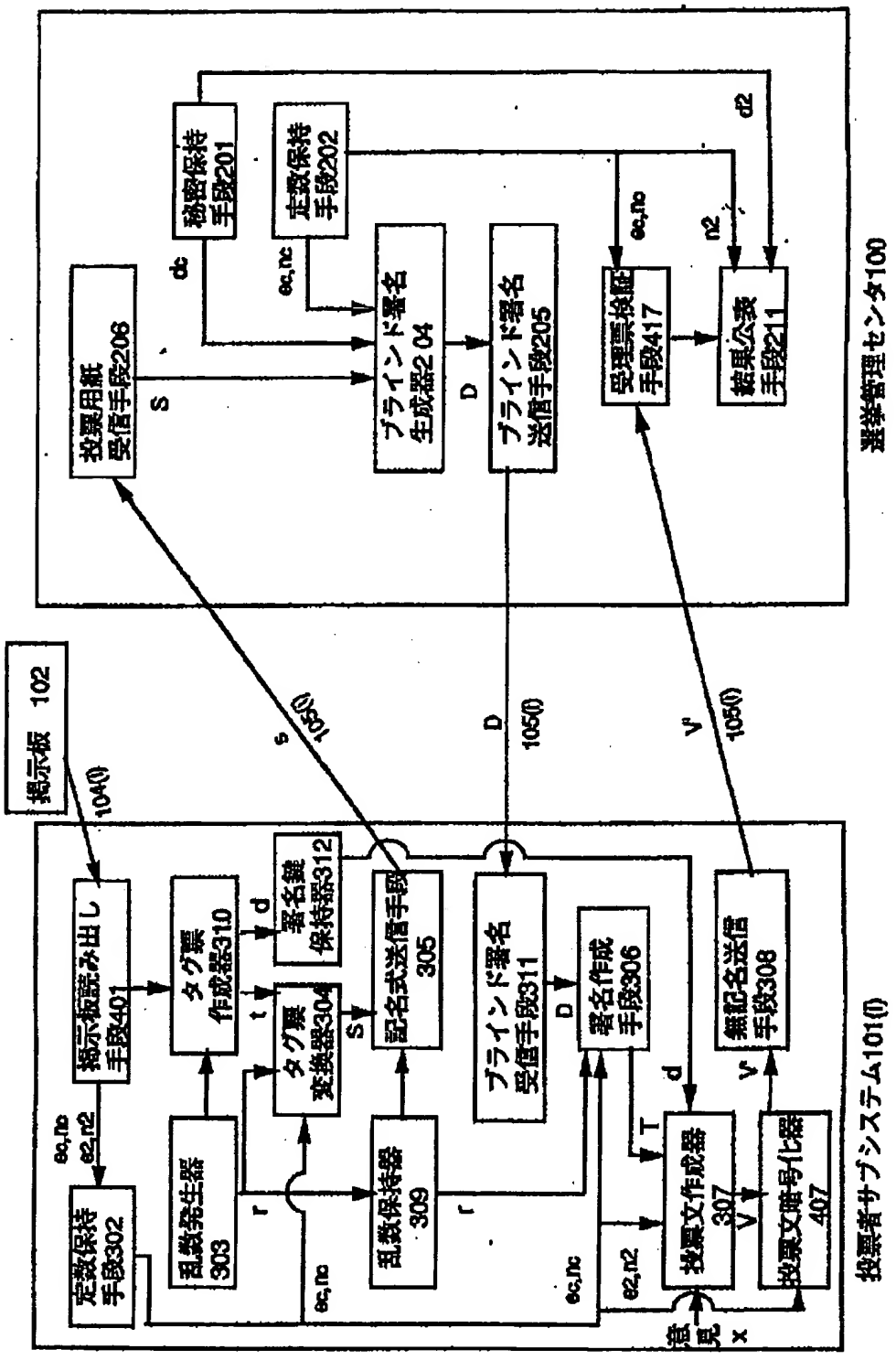
【図1】


選挙管理センタ100
秘密保持手段201
定数保持手段202
投票用紙受信手段206
ブラインド署名生成器204
ブラインド署名送信手段205
受理票検証手段207
結果公表手段211
dc
nc
ec,nc
S
D
掲示板 102
104(i)
105(i)
投票者サブシステム101(i)
掲示板読み出し手段301
定数保持手段302
乱数発生器303
タグ票作成器310
タグ票変換器304
署名鍵保持器312
配名式送信手段305
乱数保持器309
ブラインド署名受信手段311
署名作成手段306
投票文作成器307
無配名送信手段308
r
t
d
T
V
x
投票

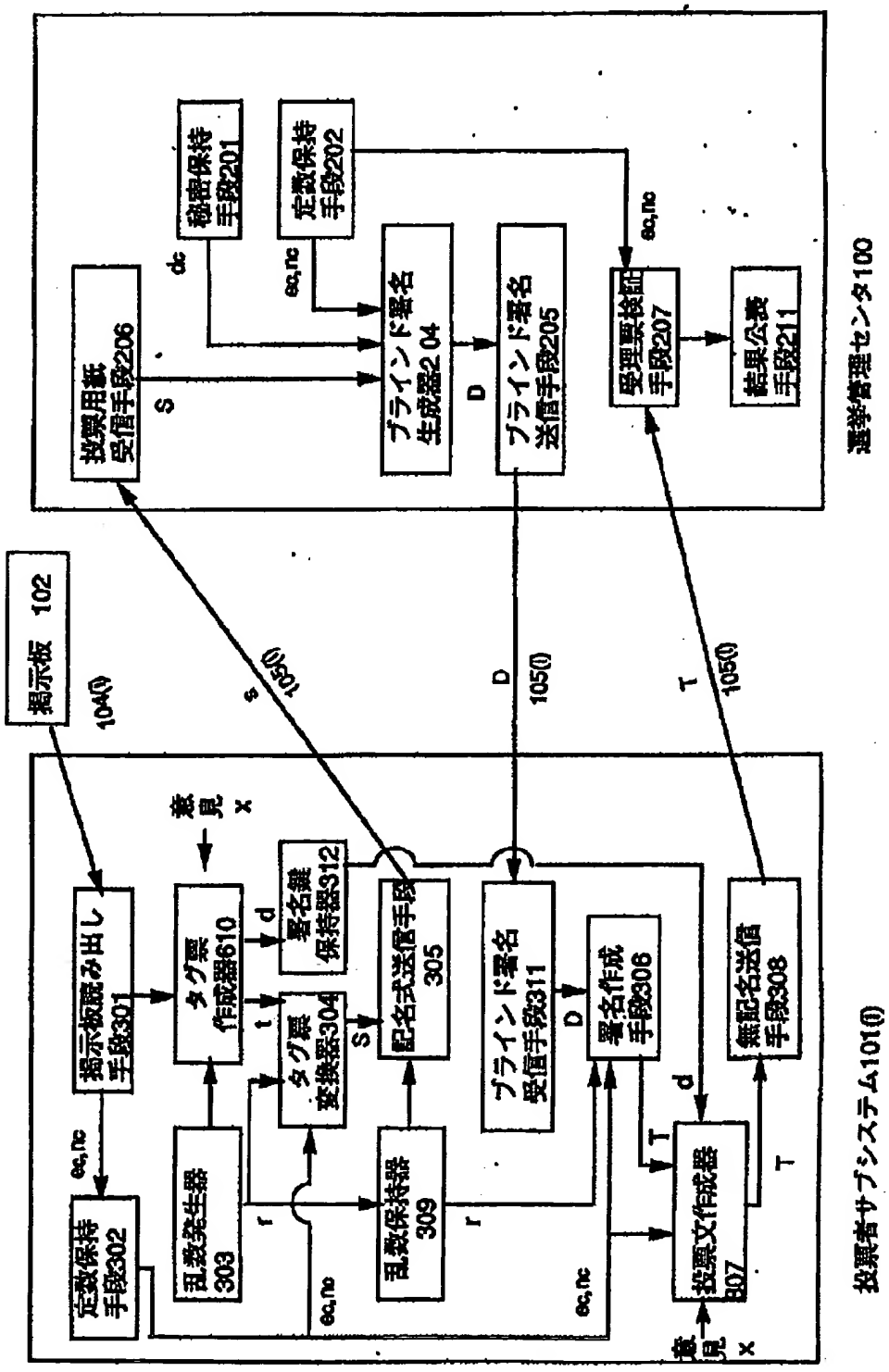
【図4】



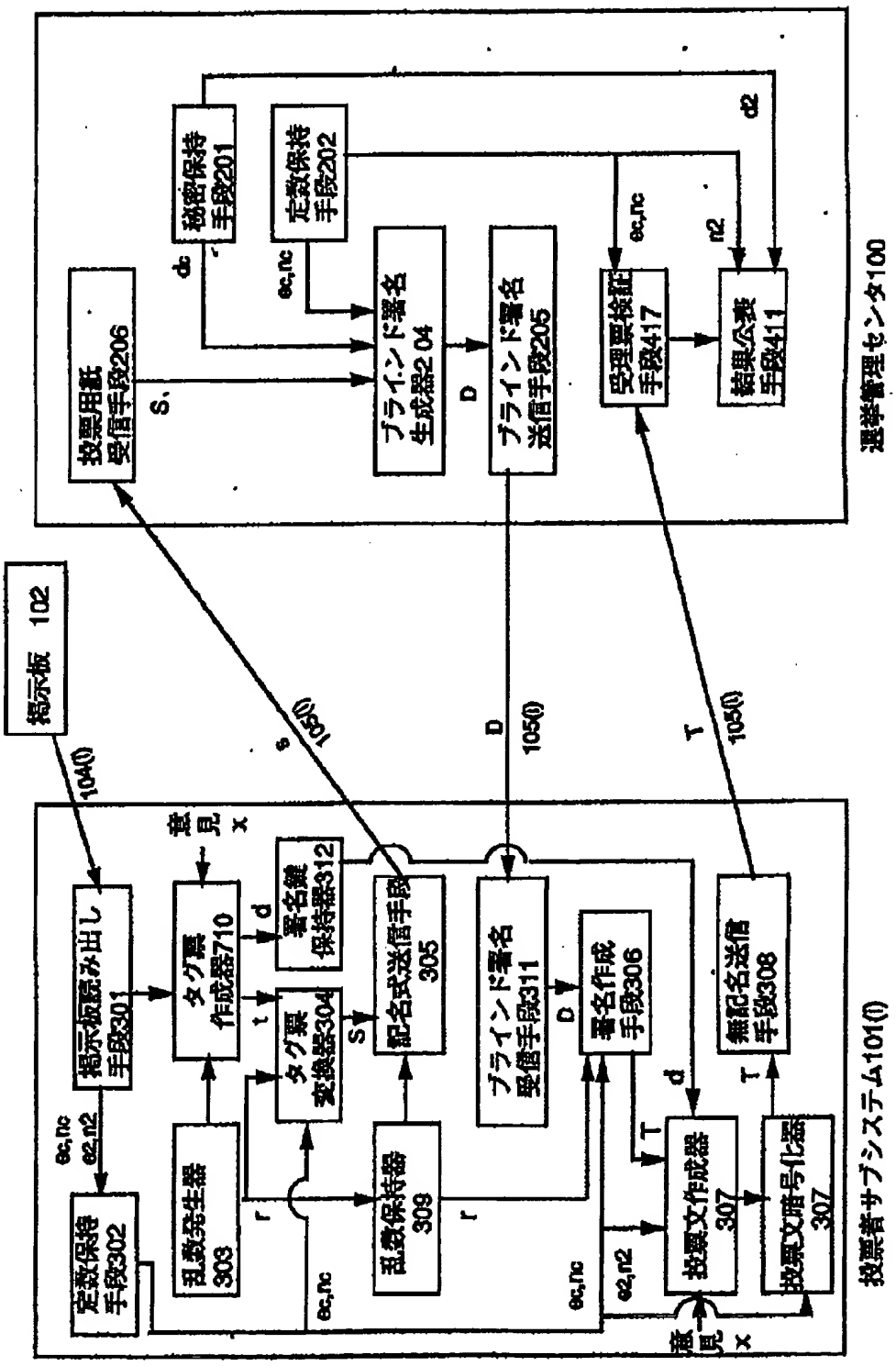
【図5】


選挙管理センタ100
秘密保持手段201
定数保持手段202
ブラインド署名生成器204
ブラインド署名送信手段205
投票用紙受信手段206
受理票検証手段417
結果公表手段211
投票者サブシステム101(i)
掲示板　102
掲示板読み出し手段401
タグ票作成器310
署名鍵保持器312
タグ票変換器304
記名式送信手段305
ブラインド署名受信手段311
署名作成手段306
無記名送信手段308
定数保持手段302
乱数発生器303
乱数保持器309
投票文作成器307
投票文暗号化器407

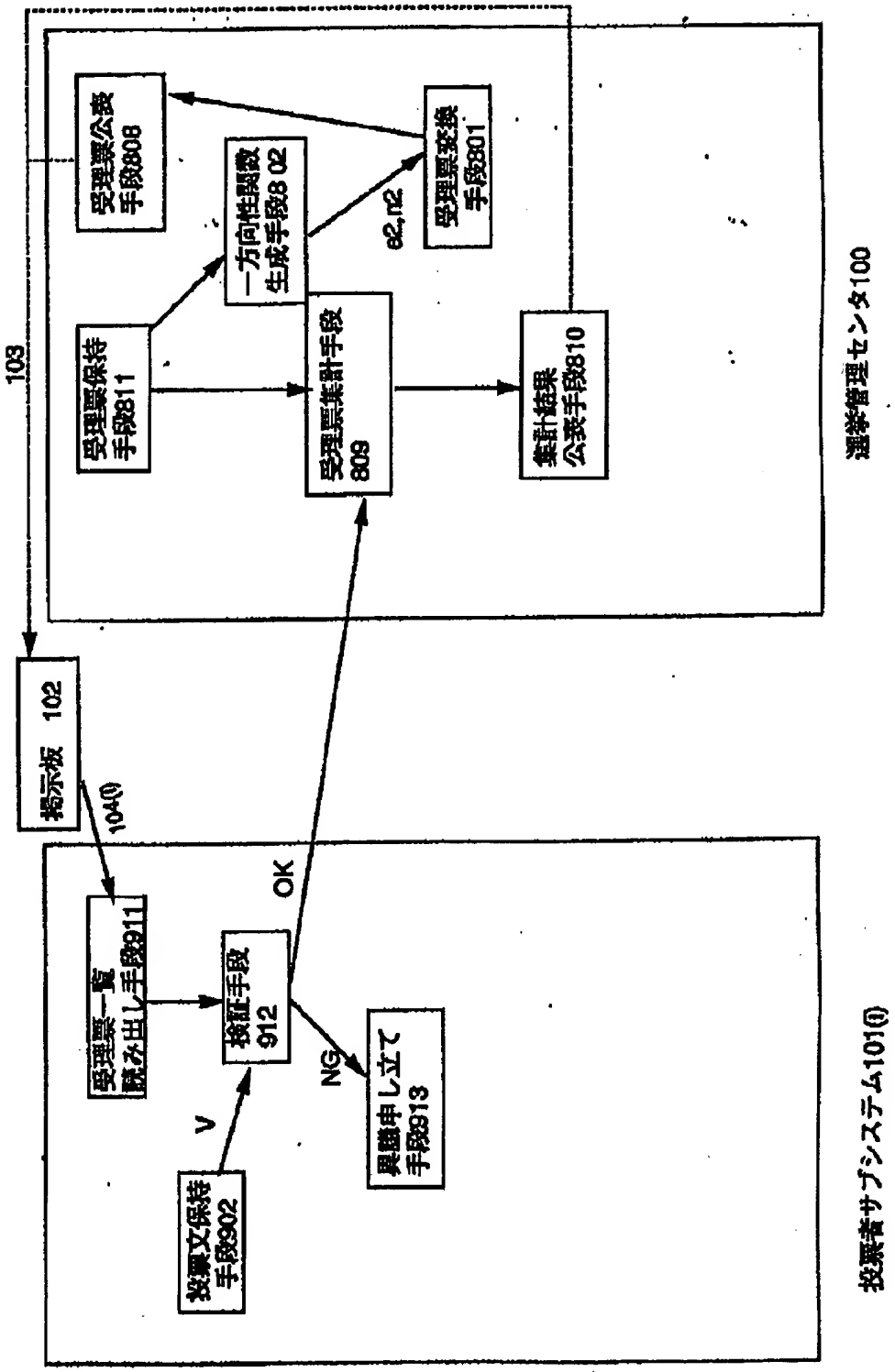
【図6】


選挙管理センタ100
投票用紙受信手段206
秘密保持手段201
定数保持手段202
ブラインド署名生成器204
ブラインド署名送信手段205
受理票検証手段207
結果公表手段211
dc
ec,nc
S
D
T
掲示板 102
104(i)
105(i)
投票者サブシステム101(i)
意見 x
掲示板読み出し手段301
タグ票作成器610
署名鍵保持器312
定数保持手段302
乱数発生器303
タグ票変換器304
記名式送信手段305
乱数保持器309
ブラインド署名受信手段311
署名作成手段306
無記名送信手段308
投票文作成器307
r
t
d

【図7】


選挙管理センタ100
投票用紙受信手段206
秘密保持手段201
定数保持手段202
ブラインド署名生成器204
ブラインド署名送信手段205
受理票検証手段417
結果公表手段411
掲示板 102
投票者サブシステム101(i)
掲示板読み出し手段301
タグ票作成器710
署名鍵保持器312
タグ票変換器304
記名式送信手段305
ブラインド署名受信手段311
署名作成手段306
無記名送信手段308
定数保持手段302
乱数発生器303
乱数保持器309
投票文作成器307
投票文暗号化器307
意見 x
1040(i)
1060(i)
1050(i)

【図8】


投票者サブシステム101(i)
選挙管理センタ100
103
掲示板　102
104(i)
受理票一覧
載み出し手段911
投票文保持
手段902
V
検証手段
912
NG
OK
異議申し立て
手段913
受理票保持
手段811
一方向性関数
生成手段802
受理票公表
手段808
受理票変換
手段801
α2,π2
受理票集計手段
809
集計結果
公表手段810